

Formal group exponentials and Galois modules in Lubin-Tate extensions

Erik Jarl Pickett and Lara Thomas

January 20, 2012

Abstract

Explicit descriptions of local integral Galois module generators in certain extensions of p -adic fields due to Pickett have recently been used to make progress with open questions on integral Galois module structure in wildly ramified extensions of number fields. In parallel, Pulita has generalised the theory of Dwork's power series to a set of power series with coefficients in Lubin-Tate extensions of \mathbb{Q}_p to establish a structure theorem for rank one solvable p -adic differential equations.

In this paper we first generalise Pulita's power series using the theories of formal group exponentials and ramified Witt vectors. Using these results and Lubin-Tate theory, we then generalise Pickett's constructions in order to give an analytic representation of integral normal basis generators for the square root of the inverse different in all abelian totally, weakly and wildly ramified extensions of a p -adic field. Other applications are also exposed.

Introduction

The main motivation for this paper came from new progress in the theory of Galois module structure. Indeed, explicit descriptions of local integral Galois module generators due to Erez [5] and Pickett [16] have recently been used to make progress with open questions on integral Galois module structure in wildly ramified extensions of number fields (see [18] and [23]).

Precisely, let p be a prime number. Pickett, generalising work of Erez, has constructed normal basis generators for the square root of the inverse different in degree p extensions of any unramified extension of \mathbb{Q}_p . His constructions were obtained by using special values of Dwork's power series. Moreover, they have recently been used by Pickett and Vinatier [18] to prove that the square root of the inverse different of E/F is free over $\mathbb{Z}[G]$ under certain conditions on both the decomposition groups of G and the base field F , when E/F is a finite odd degree Galois extension with group G .

In parallel, Pulita has generalised the theory of Dwork's power series to a set of power series with coefficients in Lubin-Tate extensions of \mathbb{Q}_p in order to classify rank one p -adic solvable differential equations [19].

Our main goal was to generalise Erez and Pickett's construction in order to give explicit descriptions of integral normal basis generators for the square root of the inverse different in all abelian totally, weakly and wildly ramified extensions of a p -adic field. In this paper, our goal is totally achieved using a combination of several tools : formal group exponentials, Lubin-Tate theory, and the theory of ramified Witt vectors. This leads us to generalise Pulita's formal power series to power series with coefficients in Lubin-Tate extensions of any finite extension of \mathbb{Q}_p .

At the same time, we also get explicit generators for the valuation ring over its associated order, in maximal abelian totally, weakly and wildly ramified extensions of any p -adic field.

Notation. Let p be a rational prime, and let \mathbb{Q}_p be the field of p -adic numbers, $\bar{\mathbb{Q}}_p$ be a fixed algebraic closure of \mathbb{Q}_p and \mathbb{C}_p be the completion of $\bar{\mathbb{Q}}_p$ with respect to the p -adic absolute value. We let v_p and $|\cdot|_p$ be the normalised p -adic valuation and absolute value on \mathbb{C}_p such that $v_p(p) = 1$ and $|x|_p = p^{-v_p(x)}$. As v_p and $|\cdot|_p$ are completely determined by each other, either can be used in the statement of results; we will use the valuation v_p as this is the convention in the literature on Galois modules in Lubin-Tate extensions.

Throughout this paper, for any extension K/\mathbb{Q}_p considered we will always assume K is contained in $\bar{\mathbb{Q}}_p$ and we will denote by \mathcal{O}_K , \mathcal{P}_K and k its valuation ring, maximal ideal and residue field respectively. We identify the residue field of \mathbb{Q}_p with the field of p elements, \mathbb{F}_p . For any $n \in \mathbb{Z}_{>0}$, we denote by μ_n the group of n th roots of unity contained in $\bar{\mathbb{Q}}_p^\times$.

Presentation of the paper. Let $\gamma \in \bar{\mathbb{Q}}_p$ be a root of the polynomial $X^{p-1} + p$. Dwork's exponential power series with respect to γ is defined as

$$E_\gamma(X) = \exp(\gamma(X - X^p)) \in 1 + X\mathbb{Z}_p[[X]],$$

where the right hand side is the composition of the two power series $\gamma(X - X^p)$ and $\exp(X)$. Dwork's power series is *over-convergent*, in the sense that it converges with respect to $|\cdot|_p$ on an open disc $\{x \in \mathbb{C}_p : v_p(x) > c\}$ for some $c < 0$ ([14], Chap. 14, §2, Remark after Lem. 2.2); it also has the property that $E_\gamma(1)$ is equal to a primitive p th root of unity in \mathbb{Q}_p ([14], Chap. 14, §3, Thm 3.2).

Dwork's power series was recently generalised by Pulita [19] to a set of power series with coefficients in Lubin-Tate extensions of \mathbb{Q}_p : Let $f(X) \in \mathbb{Z}_p[X]$ be some Lubin-Tate polynomial with respect to the uniformising parameter p , *i.e.*,

$$P(X) \equiv X^p \pmod{p\mathbb{Z}_p[X]} \quad \text{and} \quad P(X) \equiv pX \pmod{X^2\mathbb{Z}_p[X]} .$$

Let $\{\omega_i\}_{i>0}$ be a *coherent set of roots* associated to $P(X)$, namely a sequence of elements of $\bar{\mathbb{Q}}_p$ such that $\omega_1 \neq 0$, $P(\omega_1) = 0$ and $P(\omega_{i+1}) = \omega_i$; we refer to ω_n as an n th Lubin-Tate division point with respect to P . For $n \in \mathbb{Z}_{>0}$, Pulita defines the exponentials

$$E_{P,n}(X) = \exp\left(\sum_{i=0}^{n-1} \frac{\omega_{n-i}(X^{p^i} - X^{p^{i+1}})}{p^i}\right) \in 1 + X\mathbb{Z}_p[\omega_n][[X]] .$$

This generalises Dwork's power series as $E_{P,1}(X) = E_\gamma(X)$ when $P(X) = X^p + pX$. For all choices of $P(X)$ and n , the power series $E_n(X)$ is over-convergent and has the property that $E_n(1)$ is a primitive p^n th root of unity ζ_{p^n} in \mathbb{Q}_p . Comparing degrees then shows us that $\mathbb{Q}_p(\omega_n) = \mathbb{Q}_p(\zeta_{p^n})$ for all n and all choices of $P(X)$. We remark that this result is also a consequence of basic Lubin-Tate theory, see [15] or [20] for details of this theory.

In this paper, we first generalise Pulita's exponentials to power series with coefficients in Lubin-Tate extensions of any finite extension K of \mathbb{Q}_p , in particular by combining Fröhlich's notion of a formal group exponential ([7], Chap. IV, §1) with the theory of ramified Witt vectors. Note that we impose no other restrictions on our base field K and no restrictions on the uniformising parameter used to construct the Lubin-Tate extensions of K . Inspired by the methods of Pulita, we prove the following core result of the paper :

Theorem 1 *Let K be a finite extension of \mathbb{Q}_p , with valuation ring, maximal ideal and residue field denoted by \mathcal{O}_K , \mathcal{P}_K and k respectively. Let $q = \text{card}(k)$ for some power q of p .*

Let π and π' be two uniformising parameters for \mathcal{O}_K , and let $P, Q \in \mathcal{O}_K[[X]]$ be Lubin-Tate polynomials with respect to π and π' respectively, i.e.,

$$P(X) \equiv X^q \pmod{\pi \mathcal{O}_K[X]} \quad \text{and} \quad P(X) \equiv \pi X \pmod{X^2 \mathcal{O}_K[X]} .$$

We write $F_P \in \mathcal{O}_K[[X, Y]]$ for the unique formal group that admits P as an endomorphism and $\exp_{F_P} \in XK[[X]]$ for the unique power series such that

$$\exp_{F_P}(X + Y) = F_P(\exp_{F_P}(X), \exp_{F_P}(Y)).$$

Let $\{\omega_i\}_{i \geq 0}$ be a coherent set of roots associated to Q .

1. *For every $n \geq 1$, the formal power series*

$$\mathcal{E}_{P,n}^Q(X) := \exp_{F_P} \left(\sum_{i=0}^{n-1} \frac{\omega_{n-i}(X^{q^i} - X^{q^{i+1}})}{\pi^i} \right)$$

lies in $X\mathcal{O}_K[\omega_n][[X]]$, and is over-convergent if $\pi \equiv \pi' \pmod{\mathcal{P}_K^{n+1}}$.

2. *Moreover, we have the congruence $\mathcal{E}_{P,n}^Q(X) \equiv \omega_n X \pmod{\omega_n^2 X \mathcal{O}_K[\omega_n][[X]]}$.*

To compare to Pulita's result, we remark that if $K = \mathbb{Q}_p$, $\pi = \pi' = p$, and $P(X) = (X + 1)^p - 1$, then $\mathcal{E}_{P,n}^Q(X) = E_{Q,n}(X) - 1$.

We then apply Theorem 1 to give two explicit results in Lubin-Tate theory. For each integer $n \geq 1$, we denote by $K_{\pi,n}$ the n -th Lubin-Tate extension of K with respect to π . This extension is abelian and totally ramified, with degree $q^{n-1}(q-1)$ and conductor n . Let $P \in \mathcal{O}_K[X]$ be a Lubin-Tate polynomial with respect to π . The extension $K_{\pi,n}/K$ is generated by any primitive n -th Lubin-Tate division point with respect to P , i.e., any element $\omega \in \bar{\mathbb{Q}}_p$ such that $P^{(n)}(\omega) = 0$ whereas $P^{(n-1)}(\omega) \neq 0$.

As a first application of Theorem 1, we give an analytic representation of Lubin-Tate division points as values of the power series $\mathcal{E}_{P,n}^Q(X)$ for all $n \geq 0$. Precisely, keeping the same notation, we prove :

Proposition 1 *1. If $\pi \equiv \pi' \pmod{\mathcal{P}_K^{n+1}}$, then $\mathcal{E}_{P,m}^Q(1)$ is a primitive m th Lubin-Tate division point with respect to P , for all integers m with $0 < m \leq n$.*
2. If $\pi' = \pi$, then $\{\mathcal{E}_{P,i}^Q(1)\}_{i>0}$ is a coherent set of roots associated to $P(X)$.

Another application of Theorem 1 is concerned with an explicit description of the action of the Galois group $\text{Gal}(K_{\pi,n}/K)$ over the Lubin-Tate extension $K_{\pi,n}$ for all $n \geq 1$. Indeed, since $\mathcal{E}_{P,n}^Q(1)$ is a primitive n th Lubin-Tate division point with respect to P , from standard theory (see [11], §6-7, specifically Theorem 7.1) we know that the elements of $\text{Gal}(K_{\pi,n}/K)$ are those automorphisms such that $\mathcal{E}_{P,n}^Q(1) \mapsto [u]_P(\mathcal{E}_{P,n}^Q(1))$, where u runs over a set of representatives of $\mathcal{O}_K^\times / (1 + \mathcal{P}_K^n)$ — here $[u]_P(X)$ is a specific power series in $X\mathcal{O}_K[[X]]$, see Section 1.1 for full details. Therefore, the following proposition gives a complete description of $\text{Gal}(K_{\pi,n}/K)$ in terms of values of our power series.

Proposition 2 *Let $\pi \equiv \pi' \pmod{\mathcal{P}_K^{n+1}}$. For $0 \leq i \leq n-1$, let $z_i \in \mu_{q-1} \cup \{0\}$ with $z_0 \neq 0$. Then,*

$$\left[\sum_{i=0}^{n-1} z_i \pi^i \right]_P(\mathcal{E}_{P,n}^Q(1)) = \mathcal{E}_{P,n}^Q(z_0) +_{F_P} \mathcal{E}_{P,n-1}^Q(z_1) +_{F_P} \dots +_{F_P} \mathcal{E}_{P,1}^Q(z_{n-1}) .$$

Note that, when $z_1 = \dots = z_{n-1} = 0$, this proposition implies the relation

$$\mathcal{E}_{P,n}^Q(z_0) = [z_0]_P(\mathcal{E}_{P,n}^Q(1)) , \quad \text{for all } z_0 \in \mu_{q-1}.$$

This is a generalisation of ([13], Chap. 14, Thm. 3.2).

Finally, we shall prove our second main result, as a consequence of Theorem 1 and Proposition 1 : we use the power series $\mathcal{E}_{P,2}^Q(X)$ to construct explicit normal basis generators in abelian, weakly and wildly ramified extensions of any p -adic field. In this manner, we generalise the constructions of Erez and Pickett, and give support towards the resolution of open questions in Galois module structure theory :

Theorem 2 *Let K be a finite extension of \mathbb{Q}_p , with valuation ring \mathcal{O}_K , residue field k and residue cardinality q . Fix a uniformising parameter π of K and let $P(X) = X^q + \sum_{i=2}^{q-1} a_i X^i + \pi X$ be some Lubin-Tate polynomial of degree q with respect to π . Let $M_{\pi,2}$ be a maximal abelian totally, weakly and wildly ramified extension of K . Let $\mathcal{A}_{M_{\pi,2}/K}$ denote the unique fractional ideal in $M_{\pi,2}$ whose square is equal to the inverse different of $M_{\pi,2}/K$ (see Section 3.3).*

Let $\pi' \in K$ be another uniformising element of K , with $\pi \equiv \pi' \pmod{\mathfrak{p}_K^3}$; and let $Q \in \mathcal{O}_K[X]$ be a Lubin-Tate polynomial with respect to π' .

If $v_p(a_{q-1}) = v_p(\pi)$, then

1. the trace element $\text{Tr}_{K_{\pi,2}/M_{\pi,2}}(\mathcal{E}_{P,2}^Q(1))$ is a uniformising parameter of $M_{\pi,2}$ and a generator of the valuation ring $\mathcal{O}_{M_{\pi,2}}$ of $M_{\pi,2}$ over its associated order in the extension $M_{\pi,2}/K$;
2. if p is odd, then the elements

$$\frac{\text{Tr}_{K_{\pi,2}/M_{\pi,2}}(\mathcal{E}_{P,2}^Q(1))}{\pi} \quad \text{and} \quad \frac{\text{Tr}_{K_{\pi,2}/M_{\pi,2}}(\mathcal{E}_{P,2}^Q(1)) + q}{\pi}$$

are both generators of $\mathcal{A}_{M_{\pi,2}/K}$ over $\mathcal{O}_K[\text{Gal}(M_{\pi,2}/K)]$.

Furthermore, Part 2 of this theorem will enable us to give explicit integral normal basis generators for the square root of the inverse different in every abelian totally, weakly and wildly ramified extension of any p -adic field (see Corollary 3.2).

We also remark that in this second part, the first element seems the more natural, however the second is in fact the generalisation of Erez's basis generator for the square root of the inverse different. If these basis generators can be used in local calculations in a similar way to those of Erez and Pickett, it should be possible to solve the case of whether $\mathcal{A}_{E/F}$ is free over $\mathbb{Z}[G]$ whenever the decomposition groups at wild places are abelian and in particular whenever E/F itself is abelian. We hope this will be possible in the future, however, so far these calculations have eluded us.

Organisation of the paper. This paper is organised into three sections. In Section 1, we give the background to the theory we need to prove our results. Precisely, we first introduce Lubin-Tate formal groups in their original setting and also in terms of Hazewinkel's so called functional equation approach. We also introduce Fröhlich's notion of formal group exponentials and logarithms. Following work of Ditters, Drinfeld, and Fontaine and Fargues, we finally introduce the theory of ramified Witt vectors needed to generalise Pulita's methods. In Section 2, we study the properties of the power series $\mathcal{E}_{P,n}^Q(X)$ and prove Theorem 1. We also improve on Fröhlich's original bound of the radius of convergence of any formal group exponential coming from a Lubin-Tate formal group over a non-trivial extension of \mathbb{Q}_p . In Section 3, we explore the applications described above and prove Propositions 1 and 2, as well as Theorem 2.

1 Background

1.1 Formal groups

Let A be a commutative ring with identity.

Definition 1.1 We define a 1-dimensional commutative formal group over A to be a formal power series $F(X, Y) \in A[[X, Y]]$ such that

1. $F(X, Y) = F(Y, X)$
2. $F(X, F(Y, Z)) = F(F(X, Y), Z)$

$$3. F(X, 0) = X = F(0, X)$$

Throughout, all the formal groups we consider will be 1-dimensional commutative formal groups. For brevity we will now refer to these simply as formal groups.

Properties 1-3 can be used to prove that there exists a unique $j(X) \in XA[[X]]$ such that $F(X, j(X)) = 0$ (see Appendix A.4.7 of [9]). This means that the formal group $F(X, Y)$ endows $XA[[X]]$, among other sets, with an abelian group structure.

Notation 1.2 When considering a set endowed with such a group structure we write the group operation as $+_F$. We will also use the notation $-_F$ to determine this group operation composed with the group inverse, for example

$$F(X, Y) = X +_F Y \quad \text{and} \quad F(X, j(Y)) = X -_F Y .$$

Definition 1.3 Let $F(X, Y)$ and $G(X, Y)$ be two formal groups over A . A homomorphism over the ring A , $f : F(X, Y) \rightarrow G(X, Y)$, is a formal power series $f(X) \in XA[[X]]$ such that

$$f(F(X, Y)) = G(f(X), f(Y)) .$$

Moreover, we say that the homomorphism f is an isomorphism if there exists a homomorphism $f^{-1} : G(X, Y) \rightarrow F(X, Y)$ such that $f(f^{-1}(X)) = f^{-1}(f(X)) = X$.

Lubin-Tate formal groups

We now describe a special type of formal group, due originally to Lubin and Tate. Such formal groups are used in local class field theory to construct maximal totally ramified abelian extensions of a p -adic field K . For full details see, for example, [15] or [20].

Let K be a finite extension of \mathbb{Q}_p , fix a uniformising parameter π of \mathcal{O}_K and let $q = |\mathcal{O}_K/\mathcal{P}_K|$ be the cardinality of the residue field of K .

Definition 1.4 We define \mathcal{F}_π as the set of formal power series $P(X)$ over \mathcal{O}_K such that

$$P(X) \equiv \pi X \pmod{X^2 \mathcal{O}_K[[X]]} \quad \text{and} \quad P(X) \equiv X^q \pmod{\pi \mathcal{O}_K[[X]]} .$$

Such power series are called Lubin-Tate series with respect to π .

For each $P \in \mathcal{F}_\pi$ there exists a unique formal group $F_P(X, Y) \in \mathcal{O}_K[[X, Y]]$ which admits P as an endomorphism. Such formal groups are known as Lubin-Tate formal groups. For each $P \in \mathcal{F}_\pi$ and each $a \in \mathcal{O}_K$, there exists a unique formal power series, $[a]_P(X) \in X\mathcal{O}_K[[X]]$, such that $P([a]_P(X)) = [a]_P(P(X))$ and

$$[a]_P(X) \equiv aX \pmod{X^2 \mathcal{O}_K[[X]]} .$$

Further, the map $a \mapsto [a]_P(X)$ is an injective ring homomorphism $\mathcal{O}_K \rightarrow \text{End}_{\mathcal{O}_K}(F_P)$ and for any $P, Q \in \mathcal{F}_\pi$, the formal groups $F_P(X, Y)$ and $F_Q(X, Y)$ are isomorphic over \mathcal{O}_K .

Let $\mathcal{P}_{\mathbb{C}_p} = \{x \in \mathbb{C}_p : v_p(x) > 0\}$. For $P(X) \in \mathcal{F}_\pi$ and $a \in \mathcal{O}_K$, the formal power series $F_P(X, Y)$ and $[a]_P(X)$ converge to limits in $\mathcal{P}_{\mathbb{C}_p}$ when evaluated at elements of $\mathcal{P}_{\mathbb{C}_p}$. We can thus use the abelian group operation $+_F$ and the injective ring homomorphism $a \mapsto [a]_P(X)$ to endow $\mathcal{P}_{\mathbb{C}_p}$ with an \mathcal{O}_K -module structure. For every $n \geq 1$, we then let

$$T_{P,n} = \{x \in \mathcal{P}_{\mathbb{C}_p} : [\pi^n]_P(x) = 0\}$$

be the set of π^n -torsion points of this module and refer to it as the set of the n th *Lubin-Tate division points* with respect to P . If $x \in T_{P,m}$ if and only if $m \leq n$, then we say x is a primitive n th division point.

We let

$$K_{\pi,n} = K(T_{P,n}) \quad \text{and} \quad K_\pi = \cup_n K_{\pi,n} .$$

The set $T_{P,n}$ depends on the choice of the polynomial $P(X)$ but the field $K_{\pi,n}$ depends only on the uniformising parameter π . The extensions $K_{\pi,n}/K$ are totally ramified, abelian and of degree $q^{n-1}(q-1)$. We have $K^{ab} = K_\pi K^{un}$ and $K^{un} \cap K_\pi = K$, where K^{ab} and K^{un} are the maximal abelian and unramified extensions of K respectively.

Hazewinkel's approach to Lubin-Tate formal groups

We now describe a different approach to the construction of Lubin-Tate formal groups due to Hazewinkel. This approach enables us to use Hazewinkel's *functional equation lemma* to prove the integrality of various power series relating to formal groups, which will be essential in the sequel. For full details see [9] (Chap. I, §2).

Recall that p is a rational prime, K is a finite extension of \mathbb{Q}_p , π is a fixed uniformising parameter of \mathcal{O}_K and q is the cardinality of the residue field of K . For any series $g(X) \in X\mathcal{O}_K[[X]]$ we construct a new power series $f_g(X) \in XK[[X]]$ by the recursion formula (or functional equation) :

$$f_g(X) = g(X) + \frac{f_g(X^q)}{\pi} .$$

We denote by $f_g^{-1}(X) \in XK[[X]]$ the unique power series such that

$$f_g(f_g^{-1}(X)) = X = f_g^{-1}(f_g(X)) .$$

Note that if $f_g(X) \in X\mathcal{O}_K[[X]]$ and the coefficient of X in $f_g(X)$ is invertible in \mathcal{O}_K , then $f_g^{-1}(X) \in X\mathcal{O}_K[[X]]$, see [9, A.4.6].

We now state two parts of the functional equation lemma for this special setting. For the full statement in all generality and its proof, see [9, §2.2-2.4].

Theorem 1.5 (Hazewinkel, [9, 2.2]) *Let $g(X), h(X) \in X\mathcal{O}_K[[X]]$ and suppose that the coefficient of X in $g(X)$ is invertible in \mathcal{O}_K . Then,*

1. $f_g^{-1}(f_g(X) + f_g(Y)) \in \mathcal{O}_K[[X, Y]]$.
2. $f_g^{-1}(f_h(X)) \in X\mathcal{O}_K[[X]]$.

It is routine to check that $f_g^{-1}(f_g(X) + f_g(Y))$ is a formal group and from part 1. of the previous theorem we know that it has coefficients in \mathcal{O}_K . In fact, it is a Lubin-Tate formal group and every Lubin-Tate formal group can be constructed in this manner. This link is described in the following proposition.

Proposition 1.6 (Hazewinkel, [9, 8.3.6]) *Let $g(X) \in X\mathcal{O}_K[[X]]$ with*

$$g(X) \equiv X \pmod{X^2\mathcal{O}_K[[X]]}.$$

Then,

1. $f_g^{-1}(\pi f_g(X)) \in \mathcal{F}_\pi$.
2. *If we let $P(X) = f_g^{-1}(\pi f_g(X))$, then $F_P(X, Y) = f_g^{-1}(f_g(X) + f_g(Y))$.*
3. *These relations give a one to one correspondence between the Lubin-Tate formal groups obtained from power series $P(X) \in \mathcal{F}_\pi$ and power series $g(X) \in X\mathcal{O}_K[[X]]$ with $g(X) \equiv X \pmod{X^2\mathcal{O}_K[[X]]}$.*

We also observe that for any $a \in \mathcal{O}_K$, substituting $h(X) = ag(X)$ into part 2 of Theorem 1.5 then gives us $f_g^{-1}(af_g(X)) \in \mathcal{O}_K[[X]]$, and so if $P(X) = f_g^{-1}(\pi f_g(X))$, then

$$[a]_P(X) = f_g^{-1}(af_g(X)) .$$

Formal group exponentials

Hazewinkel's power series $f_g(X)$ and $f_g^{-1}(X)$ can be thought of as special formal group isomorphisms which were first studied by Fröhlich in ([7], Chap. IV, §1).

Let E be any field of characteristic 0, let $F(X, Y)$ be a formal group over E and let $\mathbb{G}_a(X, Y) = X + Y$ be the additive formal group. There exists a unique isomorphism $\log_F : F \rightarrow \mathbb{G}_a$ over E such that $\log_F(X) \equiv X \pmod{X^2E[[X]]}$, known as the formal group logarithm (*loc. cit.*, Prop. 1). The inverse of $\log_F(X)$ is known as the formal group exponential and is denoted by $\exp_F(X)$; we note that necessarily we also have, $\exp_F(X) \equiv X \pmod{X^2E[[X]]}$.

Now let $F(X, Y) = F_P(X, Y) = f_g^{-1}(f_g(X) + f_g(Y))$ be a Lubin-Tate formal group for K as in Prop. 1.6. We then have

$$f_g(X) = \log_F(X) \quad \text{and} \quad f_g^{-1}(X) = \exp_F(X) \tag{1}$$

and these power series are uniquely determined by the following equivalent identities:

$$\begin{aligned} F(X, Y) &= \exp_F(\log_F(X) + \log_F(Y)) \\ \log_F(F(X, Y)) &= \log_F(X) + \log_F(Y) \\ \exp_F(X + Y) &= F(\exp_F(X), \exp_F(Y)) \end{aligned} \tag{2}$$

We also observe that,

$$[a]_P(X) = \exp_F(a \log_F(X)) . \tag{3}$$

Remark 1.7 *The reason these power series are referred to as formal group exponentials and formal group logarithms is that if $K = \mathbb{Q}_p$, then $P(X) = (X + 1)^p - 1 \in \mathcal{F}_p$ and $F_P(X, Y) = X + Y + XY = \mathbb{G}_m$, the multiplicative formal group. We then have $\exp_{F_P}(X) = \exp(X) - 1$ and $\log_{F_P}(X) = \log(X - 1)$ where \log and \exp are the standard logarithmic and exponential power series.*

1.2 Witt vectors

This section is concerned with the notion of ramified Witt vectors, generalising the classical theory of Witt vectors introduced by Witt in his original paper [26]. This notion was first developed independently by Ditters [3] and Drinfeld [4], and then by Hazewinkel [10] from a formal group approach in a more general setting. The reader is also referred to Section 5.1 of the current preprint [12] of Fontaine and Fargues.

Standard Witt vectors

We first briefly recall the construction of “standard” Witt vectors. Let p be a prime number, and let X_0, X_1, \dots be a sequence of indeterminates. The original Witt polynomials are defined by :

$$\forall n \geq 0, \quad \mathcal{W}_n(X_0, \dots, X_n) = \sum_{i=0}^n p^i X_i^{p^{n-i}} \in \mathbb{Z}[X_0, \dots, X_n] .$$

The standard Witt vectors can be constructed as a functor $W : A \mapsto W(A)$ from the category of commutative rings to itself. Precisely, if A is a commutative ring, we first define $W(A)$ as the set of infinite sequences $A^{\mathbb{Z}_{\geq 0}}$. The elements of $W(A)$ are called Witt vectors, and to each Witt vector $x = (a_n)_n \in W(A)$, one can attach a sequence $\langle a^{(n)} \rangle_n \in A^{\mathbb{Z}_{\geq 0}}$ whose coordinates are called the *ghost components* of x and are defined by the Witt polynomials : $a^{(n)} = \mathcal{W}_n(a_0, \dots, a_n)$, for all $n \geq 0$.

The set $W(A)$ is then uniquely endowed with two laws of composition that satisfy the axioms of a commutative ring, in such a way that the *ghost map* $\Gamma_A : (a_n)_n \in W(A) \mapsto \langle a^{(n)} \rangle_n \in A^{\mathbb{Z}_{\geq 0}}$ becomes a ring homomorphism.

Under this functor, any ring homomorphism $\varphi : A \rightarrow B$ is sent to the ring homomorphism $W(\varphi) : W(A) \rightarrow W(B)$ which is defined componentwise, *i.e.*, $W(\varphi)((a_n)_n) = (\varphi(a_n))_n$. See ([1], Chap. IX) for more details.

Ramified Witt vectors

Let p be a prime number. Let K be a finite extension of \mathbb{Q}_p , with valuation ring \mathcal{O}_K and residue field k . We fix a uniformising parameter π of \mathcal{O}_K , and write $k = \mathbb{F}_q$ with $q = p^f$. Ramified Witt vectors over \mathcal{O}_K are constructed as a functor $W_{\mathcal{O}_K, \pi} : A \mapsto W_{\mathcal{O}_K, \pi}(A)$ from the category of \mathcal{O}_K -algebras to itself, starting with generalised Witt-like polynomials and then proceeding along the lines of the construction of the

usual Witt vectors. For convenience, as well as to collect some useful properties of the ramified Witt vectors, we shall briefly describe this functor.

In the case of ramified Witt vectors, the relevant polynomials are :

$$\forall n \geq 0, \quad \mathcal{W}_{n, \mathcal{O}_K, \pi}(X_0, \dots, X_n) = \sum_{i=0}^n \pi^i X_i^{q^{n-i}} \in \mathcal{O}_K[X_0, \dots, X_n] .$$

Let A be an \mathcal{O}_K -algebra. We first define $W_{\mathcal{O}_K, \pi}(A)$ as the set $A^{\mathbb{Z}_{\geq 0}}$ as the set of infinite sequences over A . We shall use the notation $(a_n)_n$ for elements in $W_{\mathcal{O}_K, \pi}(A)$, and $\langle a_n \rangle_n$ for elements in $A^{\mathbb{Z}_{\geq 0}}$.

If $(a_n)_n \in W_{\mathcal{O}_K, \pi}(A)$, we define its ghost components as $a^{(n)} = \mathcal{W}_{n, \mathcal{O}_K, \pi}(a_0, \dots, a_n)$ for all $n \geq 0$. The sequence $\langle a^{(0)}, a^{(1)}, \dots \rangle$ is called the ghost vector of $(a_n)_n$. This defines a map, that we shall denote by $\Gamma_{\pi, \mathcal{O}_K, A}$ or simply by Γ_A when the setup is explicit, called the ghost map of A :

$$\begin{aligned} \Gamma_A : W_{\mathcal{O}_K, \pi}(A) &\longrightarrow A^{\mathbb{Z}_{\geq 0}} \\ (a_n)_n &\mapsto \langle a^{(n)} \rangle_n . \end{aligned}$$

The following lemma is essential for what follows.

Lemma 1.8 *Let A be an \mathcal{O}_K -algebra with no π -torsion. Then, the ghost map Γ_A is injective. If, moreover, there exists an \mathcal{O}_K -algebra endomorphism $\sigma : A \rightarrow A$ such that $\sigma(a) \equiv a^q \pmod{\pi A}$ for all $a \in A$, then the image of Γ_A is the sub-algebra of the product algebra $A^{\mathbb{Z}_{\geq 0}}$ given by*

$$\{ \langle u_n \rangle_{n \geq 0} \in A^{\mathbb{Z}_{\geq 0}} : \sigma(u_n) \equiv u_{n+1} \pmod{\pi^{n+1} A} \} .$$

Proof. We proceed along the lines of ([1], No 2, Sect. 1, Par. 1 & 2), replacing multiplication by p by multiplication by π , and replacing p by q in the exponents. The first assertion is a consequence of the equivalence

$$(\star) \quad \Gamma_A((a_n)_n) = \langle u_n \rangle_n \Leftrightarrow \begin{cases} u_0 = a_0 \\ u_{n+1} = \mathcal{W}_{n, \mathcal{O}_K, \pi}(a_0^q, \dots, a_n^q) + \pi^{n+1} a_{n+1} . \end{cases}$$

Therefore, for every sequence $\langle u_n \rangle_n \in A^{\mathbb{Z}_{\geq 0}}$, there exists at most one element $(a_n)_n \in W_{\mathcal{O}_K, \pi}(A)$ such that $\Gamma_A((a_n)_n) = \langle u_n \rangle_n$.

The second assertion is a consequence of the following relation that can easily be proved in the same way as Lemma 1 of ([1], No 2, Sect. 1), since $q \in \pi \mathcal{O}_K$:

$$\forall x, y \in A, \forall n \geq 0, \forall m \geq 1 : \quad x \equiv y \pmod{\pi^m A} \Rightarrow x^{q^n} \equiv y^{q^n} \pmod{\pi^{m+n} A} .$$

In particular, for $m = 1$ and for any sequence $(a_n)_n \in W_{\mathcal{O}_K, \pi}(A)$, this implies that

$$\begin{aligned} \sigma(\mathcal{W}_{n, \mathcal{O}_K, \pi}(a_0, \dots, a_n)) &= \mathcal{W}_{n, \mathcal{O}_K, \pi}(\sigma(a_0), \dots, \sigma(a_n)) \\ &\equiv \mathcal{W}_{n, \mathcal{O}_K, \pi}(a_0^q, \dots, a_n^q) \pmod{\pi^{n+1} A} \\ &\equiv \mathcal{W}_{n+1, \mathcal{O}_K, \pi}(a_0, \dots, a_{n+1}) \pmod{\pi^{n+1} A} \end{aligned}$$

Therefore, according to (\star) , we can prove by iteration on $n \geq 0$ that a sequence $\langle u_n \rangle_n$ is in the image of Γ_A if and only if $\sigma(u_n) \equiv u_{n+1} \pmod{\pi^{n+1}A}$ for all n . ■

In particular, the \mathcal{O}_K -algebra $A = \mathcal{O}_K[(X_n)_n, (Y_n)_n]$, endowed with the \mathcal{O}_K -endomorphism σ given by $\sigma(X_n) = X_n^q$ and $\sigma(Y_n) = Y_n^q$, satisfies the above lemma and is such that Γ_A is bijective because the relation $\sigma(a) \equiv a^q \pmod{\pi A}$ is satisfied for all $a \in A$. Therefore, the map Γ_A transfers the structure of an \mathcal{O}_K -algebra to $W_{\mathcal{O}_K}(\mathcal{O}_K[(X_n)_n, (Y_n)_n])$. Moreover, for all $n \geq 0$ and all $x \in \mathcal{O}_K$, this defines polynomials S_n and P_n in $\mathcal{O}_K[X_0, \dots, X_n, Y_0, \dots, Y_n]$, I_n and $C_{x,n}$ in $\mathcal{O}_K[X_0, \dots, X_n]$ and F_n in $\mathcal{O}_K[X_0, \dots, X_{n+1}]$ such that

$$\begin{aligned} \Gamma_A(S_0, S_1, \dots) &= \Gamma_A(X_0, X_1, \dots) + \Gamma(Y_0, Y_1, \dots) , \\ \Gamma_A(P_0, P_1, \dots) &= \Gamma_A(X_0, X_1, \dots) \times \Gamma_A(Y_0, Y_1, \dots) , \\ \Gamma_A(C_{x,0}, C_{x,1}, \dots) &= x \cdot \Gamma_A(X_0, X_1, \dots) , \\ \Gamma_A(F_0, F_1, \dots) &= (X^{(1)}, X^{(2)}, \dots) . \end{aligned}$$

Now, for any arbitrary \mathcal{O}_K -algebra A , we endow the set $W_{\mathcal{O}_K, \pi}(A)$ with laws of composition given by

$$\forall a_n, b_n \in A, \forall x \in \mathcal{O}_K, \begin{cases} (a_n)_n + (b_n)_n &= (S_n(a_0, \dots, a_n, b_0, \dots, b_n))_n \\ (a_n)_n \times (b_n)_n &= (P_n(a_0, \dots, a_n, b_0, \dots, b_n))_n \\ x \cdot (a_n)_n &= (C_{x,n}(a_0, \dots, a_n))_n \end{cases} .$$

Moreover, if $\varphi : A' \rightarrow A$ is any homomorphism of \mathcal{O}_K -algebras, we define the map $W_{\mathcal{O}_K, \pi}(\varphi) : W_{\mathcal{O}_K, \pi}(A') \rightarrow W_{\mathcal{O}_K, \pi}(A)$ component-wise, *i.e.*, $W_{\mathcal{O}_K, \pi}(\varphi)((a_n)_n) = (\varphi(a_n))_n$. This map commutes with the previous laws of composition.

Next, for a fixed \mathcal{O}_K -algebra A , we consider the \mathcal{O}_K -algebra $B = \mathcal{O}_K[(X_a)_{a \in A}]$ which satisfies the assumptions of Lemma 1.8 with $\sigma(X_a) = X_a^q$. In particular, the ghost map Γ_B induces a bijection between $W_{\mathcal{O}_K, \pi}(B)$ and some subalgebra of $B^{\mathbb{Z}_{\geq 0}}$ that respects the previous laws of composition, which gives $W_{\mathcal{O}_K, \pi}(B)$ the structure of an \mathcal{O}_K -algebra. Now, the surjective homomorphism $\rho : X_a \in B \mapsto a \in A$ yields a surjective map $W_{\mathcal{O}_K, \pi}(\rho) : W_{\mathcal{O}_K, \pi}(B) \rightarrow W_{\mathcal{O}_K, \pi}(A)$, which endows $W_{\mathcal{O}_K, \pi}(A)$ with the structure of an \mathcal{O}_K -algebra as well, thereby proving the following:

Proposition 1.9 ([12], Lemme 5.1) *The set-valued functor $\mathcal{F} : \{\mathcal{O}_K\text{-algebras}\} \rightarrow \text{Sets}$ given by $A \mapsto A^{\mathbb{Z}_{\geq 0}}$ factors through a unique \mathcal{O}_K -algebra-valued functor*

$$W_{\mathcal{O}_K, \pi} : \{\mathcal{O}_K\text{-algebras}\} \rightarrow \{\mathcal{O}_K\text{-algebras}\}$$

such that, for any \mathcal{O}_K -algebra A , the ghost map $\Gamma_A : (a_i)_{i \geq 0} \in W_{\mathcal{O}_K, \pi}(A) \mapsto (W_{n, \mathcal{O}_K, \pi}(a_0, \dots, a_n))_{n \geq 0}$ is a homomorphism of \mathcal{O}_K -algebras.

In particular, $W_{\mathcal{O}_K, \pi}(A)$ is a \mathcal{O}_K -algebra with Witt vector $(0, 0, \dots)$ as the zero element, and Witt vector $(1, 0, 0, \dots)$ as the identity element.

An important remark is that, if π' is another uniformising parameter, there exists a unique isomorphism of functors, $u_{\pi, \pi'}$, between $W_{\mathcal{O}_K, \pi}$ and $W_{\mathcal{O}_K, \pi'}$, that commutes

with the ghost maps (see Section 5.1 of [12]). In particular, this is the reason why elements of $W_{\mathcal{O}_K, \pi}(A)$ are simply called *ramified \mathcal{O}_K -Witt vectors*.

Let A be an \mathcal{O}_K -algebra. There are three maps that play a crucial role in $W_{\mathcal{O}_K, \pi}(A)$. The first is the Teichmüller lift $[-]$, which is multiplicative and given by :

$$[-] : a \in A \mapsto [a] = (a, 0, 0, \dots) \in W_{\mathcal{O}_K, \pi}(A) .$$

The second is the Frobenius map F , defined uniquely by the polynomials F_n introduced above. Precisely, as a consequence of Lemma 1.8, one can prove that this is the unique endomorphism of the \mathcal{O}_K -algebra $W_{\mathcal{O}_K, \pi}(A)$ that satisfies :

$$\forall (a_n)_n \in W_{\mathcal{O}_K, \pi}(A), \quad \Gamma_A(F(a_0, a_1, \dots)) = \langle a^{(1)}, a^{(2)}, \dots \rangle .$$

As noticed in [12], these two maps do not depend on π , in the sense that they commute with the isomorphism $u_{\pi, \pi'}$ for any other uniformising element π' .

The last map is the Verschiebung map V_π and it is additive :

$$V_\pi : (a_n)_n \in W_{\mathcal{O}_K, \pi}(A) \mapsto (0, a_0, a_1, \dots) \in W_{\mathcal{O}_K, \pi}(A) .$$

Contrary to the others, this map depends on the choice of π . Precisely, $V_{\pi'} = \frac{\pi'}{\pi} V_\pi$. Note also the relation $\Gamma_A(V_\pi(a_0, a_1, \dots)) = \langle 0, \pi a^{(0)}, \pi a^{(1)}, \dots \rangle$.

These maps satisfy the following properties, most of which can be proved after being translated to ghost components using Lemma 1.8 :

Proposition 1.10 (([10], Thm. 6.17), ([12], §5.1)) *Let A be an \mathcal{O}_K -algebra, we have :*

- i. *The composed map FV_π is the multiplication by π in $W_{\mathcal{O}_K, \pi}(A)$, whereas the composed map $V_\pi F$ is the multiplication by $(0, 1, 0, 0, \dots)$. When A has π -torsion, these two operations correspond to each other.*
- ii. *For every $a = (a_0, a_1, \dots) \in W_{\mathcal{O}_K, \pi}(A)$, we have $F(a) \equiv a^q \pmod{\pi W_{\mathcal{O}_K, \pi}(A)}$, where a^q is the q -th power of a in $W_{\mathcal{O}_K, \pi}(A)$ and $\pi W_{\mathcal{O}_K, \pi}(A)$ is the ideal generated by $\pi(1, 0, 0, \dots)$. Moreover, if $F(a) = (\alpha_0, \alpha_1, \dots)$, then $\alpha_n \equiv a_n^q \pmod{\pi A}$ for all $n \geq 0$.*
- iii. *If l/k is a finite extension, then $W_{\mathcal{O}_K, \pi}(l)$ is the ring of integers of the unique unramified extension L/K with residue field extension l/k .*

Remark 1.11 *In the language of Hazewinkel, these ramified Witt vectors are “untwisted”. In his paper [10], Hazewinkel describes the functor of even more general Witt vectors, called “twisted ramified Witt vectors”, from a formal group law approach based on the functional equation lemma. These Witt vectors are obtained from the ramified Witt vectors by twisting the Teichmüller lift with some Lubin-Tate formal group law. Such a twist is necessary for Hazewinkel to describe all ramified discrete valuation rings with not necessarily finite residue fields. See also Section 5.1.2 of [12] for a twisted version of ramified Witt vectors.*

Link with standard Witt vectors.

Let A be an \mathcal{O}_K -algebra. When $K = \mathbb{Q}_p$ and $\pi = p$, the ramified Witt \mathbb{Z}_p -algebra $W_{\mathbb{Z}_p, p}(A)$ is, as a ring, the ring of standard Witt vectors $W(A)$. In particular, one can prove the following (see, for example, the end of Paragraph 5.1 in [12]) :

Proposition 1.12 *Let K_0 denote the maximal unramified subextension of K/\mathbb{Q}_p . If A is a perfect \mathbb{F}_q -algebra, there is a canonical isomorphism :*

$$W_{\mathcal{O}_K, \pi}(A) \rightarrow W(A) \otimes_{\mathcal{O}_{K_0}} \mathcal{O}_K ,$$

under which the Teichmüller lifts correspond to each other, and the Frobenius map in $W_{\mathcal{O}_K, \pi}(A)$ is sent to $F^f \otimes \text{Id}$, where f is the residue index of K/\mathbb{Q}_p and F denotes the standard Frobenius map in $W(A)$.

2 The power series $\mathcal{E}_{P, n}^Q(X)$

In this section we prove Theorem 1, the core result of the paper.

2.1 Specific Witt vectors

Recall that p is a prime number and K is a finite extension of \mathbb{Q}_p , with valuation ring, valuation ideal and residue field denoted by \mathcal{O}_K , \mathcal{P}_K and k respectively. We let $q = \text{card}(k)$ and fix a uniformising parameter π of \mathcal{O}_K . In this section, we follow [19, §2.1], but in our more general setting, in order to construct some specific ramified \mathcal{O}_K -Witt vectors with useful properties.

We fix a formal power series $P \in \mathcal{O}_K[[X]]$ such that

$$P(0) = 0 \quad \text{and} \quad P(X) \equiv X^q \pmod{\pi \mathcal{O}_K[[X]]} . \quad (4)$$

This series defines an endomorphism of \mathcal{O}_K -algebras :

$$\begin{aligned} \sigma_P &: \mathcal{O}_K[[X]] \rightarrow \mathcal{O}_K[[X]] \\ h(X) &\mapsto h(P(X)) \end{aligned}$$

with the property $\sigma_P(h) \equiv h^q \pmod{\pi \mathcal{O}_K[[X]]}$ for all $h \in \mathcal{O}_K[[X]]$.

The following lemma is a straightforward generalisation of the first statement of [1, Ch.IX, §1, Exercise 14] to ramified \mathcal{O}_K -Witt vectors :

Lemma 2.1 *There is a unique homomorphism of \mathcal{O}_K -algebras*

$$\begin{aligned} S_P &: \mathcal{O}_K[[X]] \longrightarrow W_{\mathcal{O}_K, \pi}(\mathcal{O}_K[[X]]) \\ h &\mapsto S_P(h) \end{aligned}$$

such that, for every $h \in \mathcal{O}_K[[X]]$, the ghost vector of $S_P(h)$ is given by

$$\langle h(X), h(P(X)), h(P(P(X))), \dots \rangle \in \mathcal{O}_K[[X]]^{\mathbb{Z}_{\geq 0}} ,$$

i.e., such that the n -th ghost component of $S_P(h)$ is $\sigma_P^n(h)$, for every $n \geq 0$.

Moreover, the homomorphism of \mathcal{O}_K -algebras S_P is also characterised by :

$$F(S_P(h)) = S_P(h(P)) .$$

Proof. According to Lemma 1.8, since the \mathcal{O}_K -algebra $A := \mathcal{O}_K[[X]]$ has no π -torsion and is endowed with the map σ_P , its ghost map $\Gamma_A : W(A) \rightarrow A^{\mathbb{Z}_{\geq 0}}$ is injective, and each sequence $\langle h(X), h(P(X)), h(P(P(X))), \dots \rangle$ is clearly in the image of Γ_A . Therefore, for every formal power series $h \in A$, there is a unique Witt vector $S_P(h) \in W_{\mathcal{O}_K, \pi}(A)$ with ghost components $\langle h(X), h(P(X)), h(P(P(X))), \dots \rangle$, thereby proving the existence of the map S_P . Finally, we prove that this is a homomorphism of \mathcal{O}_K -algebras after translating the properties of such a homomorphism in terms of ghost components, according to Lemma 1.8.

The last assertion is an easy consequence of the definition of the map F by the ghost components. ■

Now, let L be a finite extension of K . We denote by \mathcal{O}_L the valuation ring of L , and by l its residue field. Let $a \in \mathcal{O}_L$ be such that $v_p(a) > 0$. By functoriality, the specialisation $\mathcal{O}_K[[X]] \rightarrow \mathcal{O}_L$, given by $X \mapsto a$, provides a homomorphism $W_{\mathcal{O}_K, \pi}(\mathcal{O}_K[[X]]) \rightarrow W_{\mathcal{O}_K, \pi}(\mathcal{O}_L)$. For every such element $a \in \mathcal{O}_L$ and every formal power series $h \in \mathcal{O}_K[[X]]$, we shall denote by $S_{P,a}(h)$ the specialised Witt vector of $W_{\mathcal{O}_K, \pi}(\mathcal{O}_L)$ which is the image of h via the composed homomorphism

$$\begin{array}{ccc} S_P & & X \mapsto a \\ \mathcal{O}_K[[X]] & \longrightarrow & W_{\mathcal{O}_K, \pi}(\mathcal{O}_K[[X]]) \longrightarrow W_{\mathcal{O}_K, \pi}(\mathcal{O}_L) . \end{array}$$

In particular, note that the ghost vector of $S_{P,a}(h)$ is $\langle h(a), h(P(a)), h(P(P(a))), \dots \rangle$.

The following proposition is a key ingredient for what follows :

Proposition 2.2 *Let $h(X) = \sum_{i \geq 0} a_i X^i$ be a formal power series in $\mathcal{O}_K[[X]]$, let $a \in \mathcal{O}_L$ with $v_p(a) > 0$ and write $S_{P,a}(h) = (\alpha_0, \alpha_1, \dots) \in W_{\mathcal{O}_K, \pi}(\mathcal{O}_L)$. Then, the following statements hold :*

- i. $a_0 = 0$ if and only if $v_p(\alpha_i) > 0$ for all $i \geq 0$;
- ii. if $a_0 \neq 0$, then $v_p(a_0) = rv_p(\pi)$ if and only if $v_p(\alpha_i) > 0$ for all $0 \leq i < r$ and $v_p(\alpha_r) = 0$.

Proof. We follow Pulita's proof of Lemma 2.2 in ([19], Sect. 2.1). The two assertions can be recovered through the equivalence of the two following statements

- (a) $v_p(a_0) = rv_p(\pi)$,
- (b) $v_p(\alpha_i) > 0$ for all $0 \leq i < r$, and $v_p(\alpha_r) = 0$,

including the case $r = +\infty$, corresponding to $a_0 = 0$.

Given $k \geq 0$, condition 2 is equivalent to $v_p(\alpha_r^k) = 0$ and $v_p(\alpha_i^k) > 0$ for all $i < r$, which is again equivalent to condition 2 applied to the Witt vector $F^k(S_{P,a}(h))$ according to the assertion iii of Proposition 1.10.

We write $(\beta_0, \beta_1, \dots)$ for the components of the Witt vector $F^k(S_{P,a}(h))$. Its ghost vector is $\langle h(P^{(k)}(a)), h(P^{(k+1)}(a)), \dots \rangle$, where $P^{(i)}$ denotes the polynomial P composed i times.

Since $v_p(P(a)) \geq \inf(qv_p(a), v_p(\pi) + v_p(a)) \geq v_p(a) > 0$, we have that $v_p(P^{(k)}(a)) \rightarrow +\infty$ as $k \rightarrow +\infty$. In particular, if k is big enough, then $v_p(h(P^{(i)}(a))) = v_p(a_0)$ for all $i \geq k$. Therefore, for such value of k , the relations between the components of $F^k(S_{P,a}(h))$ and its ghost components give us :

$$\pi^j \beta_j = h(P^{(j+k)}(a)) - (\beta_0^{q^j} + \pi \beta_1^{q^{j-1}} + \dots + \pi^{j-1} \beta_{j-1}^{q^2}) \quad \forall j \geq 0 .$$

We thus see, by iteration on $j \geq 0$, that $v_p(a_0) = rv_p(\pi)$ if and only if $v_p(\beta_j) > 0$ for all $j < r$ and $v_p(\beta_r) = 0$, thereby proving the assertion. ■

2.2 Formal group exponentials

Again, K is a finite extension of \mathbb{Q}_p , with valuation ring \mathcal{O}_K and residue field k . We write $\text{card}(k) = q$ for some power q of p . We fix a uniformising parameter π of \mathcal{O}_K . Let $P \in \mathcal{F}_\pi$ be some Lubin-Tate series with respect to π , and denote by $F_P \in \mathcal{O}_K[[X, Y]]$ the unique formal group which admits P as an endomorphism (see Subsection 1.1). By the functional equation lemma (assertion 3 of Proposition 1.6), there exists a formal power series $g \in X\mathcal{O}_K[[X]]$ with the coefficient of X equal to 1, and such that $F_P(X, Y) = f_g^{-1}(f_g(X) + f_g(Y))$, where $f_g \in XK[[X]]$ is given by Hazewinkel's functional equation construction applied to g , with uniformising parameter π and residue cardinality q . Moreover, its composition inverse $f_g^{-1} \in XK[[X]]$ equals the exponential \exp_{F_P} of the formal group F_P :

$$f_g^{-1} = \exp_{F_P} .$$

Now let $h(X) = X \in X\mathcal{O}_K[[X]]$. Hazewinkel's functional equation construction applied to h , π and q then gives us $f_h(X) = X + \frac{X^q}{\pi} + \frac{X^{q^2}}{\pi^2} + \dots$, and according to assertion 2 of Theorem 1.5, we have $f_g^{-1}(f_h(X)) \in X\mathcal{O}_K[[X]]$. Therefore, we can make the following definition :

Definition 2.3 *Let $P \in \mathcal{O}_K[[X]]$ be a Lubin-Tate series with respect to π . We define*

$$E_P(X) := \exp_{F_P} \left(X + \frac{X^q}{\pi} + \frac{X^{q^2}}{\pi^2} + \dots \right) \in X\mathcal{O}_K[[X]] .$$

Notation 2.4 *Let F be a formal group which endows a set A with a group structure under the action $+_F$. We use the following sigma notation to denote the composition of multiple elements of A using the group law $+_F$:*

$$\sum_{j_0 \leq j \leq j_n}^F a_j = a_{j_0} +_F a_{j_0+1} +_F \dots +_F a_{j_n} ,$$

where $j_0 \in \mathbb{Z}_{\geq 0}$ and $j_n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$. Analogously to usual sums, the limits of infinite formal group sums might not always exist, and when they do, they might not be contained in A .

Let L be a finite extension of K . We provide the group $X\mathcal{O}_L[[X]]$ with the “ X -adic” topology induced by that of $\mathcal{O}_L[[X]]$. By what precedes, if $\lambda = (\lambda_0, \lambda_1, \dots) \in W_{\mathcal{O}_K, \pi}(\mathcal{O}_L)$, the sum with respect to the formal group law $\sum_{0 \leq j \leq \infty}^{F_P} E_P(\lambda_j X^{q^j})$ defines a formal power series in $X\mathcal{O}_L[[X]]$. Generalising the Artin-Hasse exponential relative to ramified Witt vectors by the use of formal groups, we thus define :

Definition 2.5 *For every $\lambda \in W_{\mathcal{O}_K, \pi}(\mathcal{O}_L)$, the generalised Artin-Hasse exponential relative to λ and P is*

$$E_P(\lambda, X) := \sum_{0 \leq j \leq \infty}^{F_P} E_P(\lambda_j X^{q^j}) = \exp_{F_P} \left(\lambda^{(0)} X + \lambda^{(1)} \frac{X^q}{\pi} + \lambda^{(2)} \frac{X^{q^2}}{\pi^2} + \dots \right) \in X\mathcal{O}_L[[X]] .$$

We then fix another uniformising parameter for \mathcal{O}_K , denoted by π' , and let $Q \in \mathcal{O}_K[[X]]$ be a Lubin-Tate series with respect to π' . We fix a coherent set of roots $\{\omega_i\}_{i \geq 0}$ associated to $Q(X)$, i.e., a sequence of elements of \mathbb{Q}_p such that $\omega_1 \neq 0$, $Q(\omega_1) = 0$ and $Q(\omega_{i+1}) = \omega_i$.

We also fix $n \geq 1$ and let $L = K_{\pi', n}$ be the n th Lubin-Tate extension of K with respect to π' . We note that $\mathcal{O}_L = \mathcal{O}_K[\omega_n]$. Let $h(X) = X$. Since π and π' generate the same ideal in \mathcal{O}_K , the polynomial Q satisfies Identities 4. In particular, according to Lemma 1.8 and Section 2.1, the Witt vector $S_{Q, \omega_n}(h)$ is well defined in $W_{\mathcal{O}_K, \pi}(\mathcal{O}_L)$ for every $n \geq 1$, and it is the unique Witt vector in $W_{\mathcal{O}_K, \pi}(\mathcal{O}_L)$ with ghost vector $\langle \omega_n, \omega_{n-1}, \dots, \omega_1, 0, \dots \rangle \in \mathcal{O}_L^{\mathbb{Z}_{\geq 0}}$.

Definition 2.6 *We define*

$$E_{P, n}^Q(X) := E_P(S_{Q, \omega_n}(h), X) \in X\mathcal{O}_L[[X]] ,$$

for $h(X) = X \in X\mathcal{O}_L[[X]]$.

As an interesting consequence of the properties of these power series, we can give an improvement to the known bound for the radius of convergence of the formal group exponential $\exp_{F_P}(X)$.

Proposition 2.7 *The power series $\exp_{F_P}(X)$ converges on the disc $\{x \in \mathbb{C}_p : v_p(x) > 1/e_K(q-1)\}$, where $e_K = v_\pi(p)$ denotes the absolute ramification index of K if v_π is the discrete valuation on K such that $v_\pi(\pi) = 1$.*

Proof. First, with $h(X) = X$, we know $\exp_{F_P}(\omega_1 X) = E_P(S_{Q,\omega_1}(h), X) = E_{P,1}^Q(X)$ is a formal power series with integral coefficients, so it converges at any element $x \in \mathbb{C}_p$ with strictly positive valuation. We know that $v_p(\omega_1) = 1/(q-1)e_K$ as ω_1 is a uniformising parameter for $K_{\pi',1}$, therefore $\exp_{F_P}(x)$ converges whenever $v_p(x) > 1/(q-1)e_K$. ■

Remark 2.8 *The only bound of the radius of convergence of $\exp_{F_P}(X)$ known to the authors was that given by Fröhlich in [7, Ch.IV, Thm 3], which he accredits to Serre. This bound was $1/(p-1)$, so our bound improves this result for all $K \neq \mathbb{Q}_p$. For $K = \mathbb{Q}_p$ and $P(X) = (X+1)^p - 1$, we obtain $\exp_{F_P}(X) = \exp(X) - 1$ and we see that this bound is optimal. We conjecture that this bound is in fact optimal for all choices of K and P .*

One crucial argument in the proof of Theorem 1 will be provided by the following lemma :

Lemma 2.9 *Let $h(X) = X$. For every $\lambda = (\lambda_0, \lambda_1, \dots) \in W_{\mathcal{O}_K, \pi}(\mathcal{O}_L)$, the following equality holds ;*

$$E_P(S_{Q,\omega_n}(h)\lambda, X) = \sum_{0 \leq j \leq n-1}^{F_P} E_{P,n-j}^Q(\lambda_j X^{q^j}) .$$

Proof. On the one hand, using Definition 2.5 and the multiplicativity of the ghost map for ramified Witt vectors, we get successively :

$$\begin{aligned} E_P(S_{Q,\omega_n}(h)\lambda, X) &= \exp_{F_P} \left(\omega_n \lambda^{(0)} X + \omega_{n-1} \lambda^{(1)} \frac{X^q}{\pi} + \dots + \omega_1 \lambda^{(n-1)} \frac{X^{q^{n-1}}}{\pi^{n-1}} \right) \\ &= \exp_{F_P} \left(\sum_{0 \leq l \leq n-1} \omega_{n-l} \sum_{0 \leq j \leq l} \lambda_j^{q^{l-j}} \frac{X^{q^l}}{\pi^{l-j}} \right) \\ &= \exp_{F_P} \left(\sum_{0 \leq j \leq n-1} \sum_{0 \leq k \leq n-1-j} \omega_{n-j-k} \lambda_j^{q^k} \frac{X^{q^{j+k}}}{\pi^k} \right) \end{aligned}$$

On the other hand, using Definition 2.6, Definition 2.5 and Identities 2, we also get :

$$\begin{aligned} \sum_{0 \leq j \leq n-1}^{F_P} E_{P,n-j}^Q(\lambda_j X^{q^j}) &= \sum_{0 \leq j \leq n-1}^{F_P} E_P(S_{Q,\omega_{n-j}}(h), \lambda_j X^{q^j}) \\ &= \sum_{0 \leq j \leq n-1}^{F_P} \exp_{F_P} \left(\omega_{n-j} \lambda_j X^{q^j} + \omega_{n-j-1} \lambda_j^q \frac{X^{q^{j+1}}}{\pi} + \dots + \omega_1 \lambda_j^{q^{n-j-1}} \frac{X^{q^{n-1}}}{\pi^{n-j-1}} \right) \\ &= \exp_{F_P} \left(\sum_{0 \leq j \leq n-1} \sum_{0 \leq k \leq n-j-1} \omega_{n-j-k} \lambda_j^{q^k} \frac{X^{q^{j+k}}}{\pi^k} \right), \end{aligned}$$

thereby proving the desired equality. ■

Proposition 2.10 *Let $h(X) = X \in \mathcal{O}_K[[X]]$. For every Witt vector $\lambda = (\lambda_0, \lambda_1, \dots) \in W_{\mathcal{O}_K, \pi}(\mathcal{O}_L)$, if $v_p(\lambda_i) > 0$ for all $i \in \{0, \dots, n\}$, the series $E_P(S_{Q,\omega_n}(h)\lambda, X)$ is over-convergent, i.e., it converges on the closed disk $\mathbb{D} = \{x \in \mathbb{C}_p, v_p(x) \geq 0\}$. Moreover, $E_P(S_{Q,\omega_n}(h)\lambda, x)$ has strictly positive valuation for all $x \in \mathbb{D}$.*

Proof. According to Lemma 2.9, the series $E_P(S_{Q,\omega_n}(h)\lambda, X)$ is a finite sum with respect to the formal group law F_P . Therefore, it is over-convergent if and only if each term of the sum is over-convergent and has strictly positive valuation when evaluated at $x \in \mathbb{C}_p$ with $v_p(x) \geq 0$. But this is a consequence of the property that $E_{P,n-j}^Q(\lambda_j X^{q^j}) \in \lambda_j X^{q^j} \mathcal{O}_K[[X]]$. The last assertion is therefore trivial. ■

2.3 Proof of Theorem 1

We can now prove our main theorem on the properties of the formal power series $\mathcal{E}_{P,n}^Q(X)$:

Proof of Theorem 1.

Part 1. According to identity 2 of Subsection 1.1, we have

$$\begin{aligned} \mathcal{E}_{P,n}^Q(X) &= \exp_{F_P} \left(\sum_{i=0}^{n-1} \frac{\omega_{n-i}(X^{q^i} - X^{q^{i+1}})}{\pi^i} \right) \\ &= \exp_{F_P}(\pi\omega_{n+1}X) +_{F_P} \exp_{F_P} \left(\sum_{i=0}^n \omega_{n+1-i} \left(\frac{\omega_{n-i}}{\omega_{n+1-i}} - \pi \right) \frac{X^{q^i}}{\pi^i} \right) \\ &= \exp_{F_P}(\pi\omega_{n+1}X) +_F E_P(S_{Q,\omega_{n+1}}(h)\lambda, X) \end{aligned} \quad (5)$$

with $h(X) = X$ and $\lambda = S_{Q,\omega_{n+1}}(f)$ for $f(X) = \frac{Q(X)}{X} - \pi$.

We have to prove that each term in this sum is over-convergent and has strictly positive valuation when evaluated at some $x \in \mathbb{C}_p$ with $v_p(x) \geq 0$.

We write $\lambda = (\lambda_0, \lambda_1, \dots)$. First, the constant term of $f(X)$ is $\pi' - \pi$. Therefore, if $\pi \equiv \pi' \pmod{\mathcal{P}_K^{n+1}}$, then $v_p(\lambda_i) > 0$ for all $i \in \{0, \dots, n\}$ by Proposition 2.2. So, according to Proposition 2.10, the series $E_P(S_{Q,\omega_{n+1}}(h)\lambda, X)$, which lies in $X\mathcal{O}_K[\omega_{n+1}][[X]]$, is over-convergent and has strictly positive valuation when evaluated at any x with $v_p(x) \geq 0$.

On the other hand, we know from the proof of Proposition 2.7 and Definition 2.6 that $\exp_{F_P}(\omega_1 X) \in X\mathcal{O}_K[\omega_1][[X]]$. Substituting X with $(\pi\omega_{n+1}/\omega_1)X$ and noting that $v_p(\pi) > v_p(\omega_1)$, we then see that the series $\exp_{F_P}(\pi\omega_{n+1}X)$ belongs to $(\pi\omega_{n+1}/\omega_1)X\mathcal{O}_K[\omega_{n+1}][[X]]$. In particular, it is over-convergent by Proposition 2.7, and it has positive valuation when evaluated at any x with $v_p(x) \geq 0$.

Therefore, the series $\mathcal{E}_{P,n}^Q(X)$ lies in $X\mathcal{O}_K[\omega_{n+1}][[X]]$, and thus in $X\mathcal{O}_K[\omega_n][[X]]$, since it belongs to $K_{\pi,n}[[X]]$ by definition. Moreover, it is over-convergent if $\pi \equiv \pi' \pmod{\mathcal{P}_K^{n+1}}$, thereby proving Part 1.

Part 2.

In Part 1, we saw that $\exp_{F_P}(\pi\omega_{n+1}X) \in (\pi\omega_{n+1}/\omega_1)X\mathcal{O}_K[\omega_{n+1}][[X]]$. We know that $v_p(\pi\omega_{n+1}/\omega_1) > v_p(\omega_n)$, therefore using expression (5) above and the fact that $F_P \in \mathcal{O}_K[[X, Y]]$ we are left with showing $E_P(S_{Q,\omega_{n+1}}(h)\lambda, X) \equiv \omega_n X \pmod{\omega_n^2 X\mathcal{O}_K[\omega_{n+1}][[X]]}$.

Let \mathcal{O}_L be the valuation ring of some finite extension L of K . Let $\nu = (\nu_i)_i \in W_{\mathcal{O}_K, \pi}(\mathcal{O}_L)$ and suppose that, for some j , $v_p(\nu_i) \geq v_p(\nu_j)$ for all $i \in \mathbb{Z}$. In Definition 2.3 we saw that $E_P(X) \in X\mathcal{O}_K[[X]]$. Therefore, from Definition 2.5 and the fact that $F_P(X, Y)$ has integral coefficients, we see that $E_P(\nu, X) \in \nu_j X \mathcal{O}_L[[X]]$.

In particular, let $L = K(\omega_m) = K_{\pi', m}$ for some m with $0 < m \leq n$. For $\nu = S_{Q, \omega_m}(X)$, we know from Proposition 2.2 that $v_p(\nu_i) > 0$ for all i . As $\nu \in W_{\mathcal{O}_K, \pi}(\mathcal{O}_K[\omega_m])$ we must then have $v_p(\nu_i) \geq v_p(\omega_m)$ for all i , and so

$$E_{P, j}^Q(X) = E_P(S_{P, \omega_j}(X), X) \in \omega_j X \mathcal{O}_K[\omega_j][[X]] .$$

Recall from Part 1 that $\lambda = (\lambda_i)_i = S_{Q, \omega_{n+1}}(f)$ with $f(X) = \frac{Q(X)}{X} - \pi$ and that $v_p(\lambda_i) > 0$ for all $i \in \{0, \dots, n\}$. Therefore, for $i \in \{0, \dots, n\}$ we have $v_p(\lambda_i) \geq v_p(\omega_{n+1})$, as $\lambda \in W_{\mathcal{O}_K, \pi'}(\mathcal{O}_K[\omega_{n+1}])$. We then have

$$E_{P, n+1-j}^Q(\lambda_j X^{q^j}) \in \lambda_j \omega_{n+1-j} X \mathcal{O}_K[\omega_{n+1-j}][[X]] .$$

For all $1 \leq j \leq n$ we have $v_p(\lambda_j \omega_{n+1-j}) > v_p(\omega_n)$ and from Lemma 2.9 we know that

$$E_P(S_{P, \omega_{n+1}}(X) \lambda, X) = \sum_{0 \leq j \leq n}^{F_P} E_{P, n+1-j}^Q(\lambda_j X^{q^j}) .$$

It is therefore sufficient to prove that $E_{P, n+1}^Q(\lambda_0 X) \equiv \omega_n X \pmod{\omega_n \omega_{n+1} \mathcal{O}_K[\omega_{n+1}][[X]]}$.

By definition the coefficient of X in the formal group exponential $\exp_{F_P}(X)$ is equal to 1. Therefore, if

$$E_{P, n+1}^Q(X) = \exp_{F_P} \left(\omega_{n+1} X + \omega_n \frac{X^q}{\pi} + \dots + \omega_1 \frac{X^{q^n}}{\pi^n} \right) = \sum_{i \geq 1} a_i X^i ,$$

then $a_1 = \omega_{n+1}$. Recall that $a_i \in \omega_{n+1} \mathcal{O}_K[\omega_{n+1}][[X]]$, thus

$$\begin{aligned} E_{P, n+1}^Q(\lambda_0 X) &\equiv a_1 \lambda_0 X \pmod{\omega_{n+1} \lambda_0^2 \mathcal{O}_K[\omega_{n+1}][[X]]} \\ &\equiv \omega_{n+1} \lambda_0 X \pmod{\omega_{n+1} \lambda_0^2 \mathcal{O}_K[\omega_{n+1}][[X]]} . \end{aligned}$$

By definition, we see that $\lambda_0 = \lambda^{(0)} = f(\omega_{n+1}) = \omega_n / \omega_{n+1} - \pi$, and so

$$E_{P, n+1}^Q(X) \equiv \omega_n X \pmod{(\omega_n^2 / \omega_{n+1}) \mathcal{O}_K[\omega_{n+1}][[X]]} ,$$

which proves the result since $v_p(\omega_n) > v_p(\omega_{n+1})$ and since $\mathcal{E}_{P, n}^Q \in X \mathcal{O}_K[\omega_n][[X]]$. ■

3 Applications

We recall that p is a rational prime, K is a finite extension of \mathbb{Q}_p , π and π' are uniformising parameters of \mathcal{O}_K and q is the cardinality of the residue field of K . We let $P \in \mathcal{F}_\pi$ (resp. $Q \in \mathcal{F}_{\pi'}$) be Lubin-Tate series with respect to π (resp. π'), and $F_P(X, Y)$ (resp. $F_Q(X, Y)$) be the unique formal group with coefficients in \mathcal{O}_K that admits P (resp. Q) as an endomorphism.

3.1 Lubin-Tate division points

Since the extensions $K_{\pi,n}$ are finite and abelian over K for all choices of n and π , we have $K_{\pi',n} = K_{\pi,n}$ exactly when their norm groups are equal [25, Appendix, Theorem 9]. An exact description of the norm group $N_{K_{\pi,n}/K}(K_{\pi,n}^\times)$ was computed in [11, Proposition 5.16]. Namely, $N_{K_{\pi,n}/K}(K_{\pi,n}^\times) = \langle \pi \rangle \times 1 + \mathcal{P}_K^n$. This implies $K_{\pi,n} = K_{\pi',n}$ if and only if $\pi \equiv \pi' \pmod{\mathcal{P}_K^{n+1}}$.

We now prove Proposition 1, which shows how values of the power series $\mathcal{E}_{P,n}^Q(X)$ give expressions for any n th Lubin-Tate division point with respect to P in terms of n th Lubin-Tate division points with respect to Q whenever $\pi \equiv \pi' \pmod{\mathcal{P}_K^{n+1}}$.

Proof of Proposition 1. We assume that $\pi \equiv \pi' \pmod{\mathcal{P}_K^{n+1}}$. We proceed by induction on m , with $0 < m \leq n$.

From Identities 2 and 3 of Subsection 1.1, we have

$$\begin{aligned} [\pi]_P \left(\mathcal{E}_{P,1}^Q(X) \right) &= [\pi]_P \left(\exp_{F_P}(\omega_1(X - X^q)) \right) \\ &= \exp_{F_P}(\pi \omega_1(X - X^q)) \\ &= \exp_{F_P}(\pi \omega_1 X) -_{F_P} \exp_{F_P}(\pi \omega_1 X^q) . \end{aligned}$$

From Proposition 2.7 we know that $\exp_{F_P}(X)$ converges on the disc $\{x \in \mathbb{C}_p : v_p(x) > 1/e_K(q-1)\}$. Also, in the proof of Proposition 2.7 and according to Definition 2.6, we saw that $\exp_{F_P}(\omega_1 X) \in X\mathcal{O}_K[\omega_1][[X]]$, and so $\exp_{F_P}(\pi \omega_1)$ will have positive valuation. We can therefore evaluate both the left and right hand side above at 1 and get :

$$[\pi]_P \left(\mathcal{E}_{P,1}^Q(1) \right) = \exp_{F_P}(\pi \omega_1) -_{F_P} \exp_{F_P}(\pi \omega_1) = 0 .$$

Therefore, $\mathcal{E}_{P,1}^Q(1)$ is a $[\pi]_P$ -division point. Moreover, from Theorem 1 Part 2 we know that $\mathcal{E}_{P,1}^Q(X) \equiv \omega_1 X \pmod{\omega_1^2 X \mathcal{O}_K[\omega_1][[X]]}$, and so this division point is primitive.

Now let $k \leq m$ and assume the result holds for $m = 1, \dots, k-1$. Again, using Identities 2 and 3, we have

$$\begin{aligned} [\pi]_P \left(\mathcal{E}_{P,m}^Q(X) \right) &= [\pi]_P \left(\exp_{F_P} \left(\sum_{i=0}^{m-1} \frac{\omega_{m-i}(X^{q^i} - X^{q^{i+1}})}{\pi^i} \right) \right) \\ &= \exp_{F_P} \left(\sum_{i=0}^{m-1} \frac{\pi \omega_{m-i}(X^{q^i} - X^{q^{i+1}})}{\pi^i} \right) \\ &= \exp_{F_P} \left(\pi \omega_m(X - X^q) + \sum_{i=1}^{m-1} \frac{\omega_{m-i}(X^{q^i} - X^{q^{i+1}})}{\pi^{i-1}} \right) \\ &= \exp_{F_P} \left(\pi \omega_m(X - X^q) + \sum_{i=0}^{(m-1)-1} \frac{\omega_{(m-1)-i}(X^{q^{i+1}} - X^{q^{i+2}})}{\pi^i} \right) \\ &= \exp_{F_P}(\pi \omega_m X) -_{F_P} \exp_{F_P}(\pi \omega_m X^q) +_{F_P} \mathcal{E}_{P,m-1}^Q(X^q) . \end{aligned}$$

From Theorem 1 Part 1 we know that if $\pi \equiv \pi' \pmod{\mathcal{P}_K^{n+1}}$, then $\mathcal{E}_{P,m-1}^Q(X^q)$ is over-convergent. From Proposition 2.7 we know that $\exp_{F_P}(X)$ converges on the disc $\{x \in \mathbb{C}_p : v_p(x) > 1/e_K(q-1)\}$. Therefore, all the power series on the right hand side of this equation are overconvergent. Also, $\exp_{F_P}(\pi\omega_m)$ and $\mathcal{E}_{P,m-1}^Q(1)$ both have positive valuations, so the formal group operations on these values are well defined. We can therefore evaluate both the left and right hand side at 1 :

$$[\pi]_P \left(\mathcal{E}_{P,m}^Q(1) \right) = \exp_{F_P}(\pi\omega_m) -_{F_P} \exp_{F_P}(\pi\omega_m) +_{F_P} \mathcal{E}_{P,m-1}^Q(1) = \mathcal{E}_{P,m-1}^Q(1) . \quad (6)$$

By the induction hypothesis, we know that $\mathcal{E}_{P,m-1}^Q(1)$ is a primitive $[\pi^{m-1}]_P$ -division point and therefore $\mathcal{E}_{P,m}^Q(1)$ is a primitive $[\pi^m]_P$ -division point. Part 1 now follows by induction.

Part 2 then follows directly from Part 1 and Equation 6 above. ■

3.2 Galois action on $\mathcal{E}_{P,n}^Q(1)$

From Proposition 1 we know that $K_{\pi,n} = K(\mathcal{E}_{P,n}^Q(1))$. We will now give a complete description of how $\text{Gal}(K_{\pi,n}/K)$ acts on $\mathcal{E}_{P,n}^Q(1)$.

We know that $\mathcal{E}_{P,n}^Q(1)$ is a primitive n th Lubin-Tate division point with respect to P . From standard theory (see [11, §6-7], specifically Theorem 7.1) we know that the elements of $\text{Gal}(K_{\pi,n}/K)$ are those automorphisms such that $\mathcal{E}_{P,n}^Q(1) \mapsto [u]_P(\mathcal{E}_{P,n}^Q(1))$, where u runs over a set of representatives of $\mathcal{O}_K^\times/(1 + \mathcal{P}_K^n)$, for example

$$\left\{ \sum_{i=0}^{n-1} z_i \pi^i : z_i \in \mu_{q-1} \cup \{0\}, z_0 \neq 0 \right\} .$$

We now prove Proposition 2, which gives us a complete description of $\text{Gal}(K_{\pi,n}/K)$ in terms of values of our power series.

Proof of Proposition 2. From the definition of $\mathcal{E}_{P,n}^Q(X)$ and Identity 3 of Subsection 1.1, we have

$$\begin{aligned} \left[\sum_{i=0}^{n-1} z_i \pi^i \right]_P (\mathcal{E}_{P,n}^Q(X)) &= \left[\sum_{i=0}^{n-1} z_i \pi^i \right]_P \left(\exp_{F_P} \left(\sum_{i=0}^{n-1} \frac{\omega_{n-i}(X^{q^i} - X^{q^{i+1}})}{\pi^i} \right) \right) \\ &= \exp_{F_P} \left(\left(\sum_{j=0}^{n-1} z_j \pi^j \right) \sum_{i=0}^{n-1} \frac{\omega_{n-i}(X^{q^i} - X^{q^{i+1}})}{\pi^i} \right) . \end{aligned}$$

Using Identity 2 and the observation that $z_j = z_j^{q^i}$ for all i and j , we then see that this is equal to

$$\sum_{0 \leq j \leq n-1}^{F_P} \exp_{F_P} \left(\sum_{i=0}^{n-1} \frac{\omega_{n-i}((z_j X)^{q^i} - (z_j X)^{q^{i+1}})}{\pi^{i-j}} \right) . \quad (7)$$

We now develop each term of this expression. For all $1 \leq j \leq n-1$, we get :

$$\exp_{F_P} \left(\sum_{i=0}^{n-1} \frac{\omega_{n-i}((z_j X)^{q^i} - (z_j X)^{q^{i+1}})}{\pi^{i-j}} \right) \quad (8)$$

$$\begin{aligned} &= \exp_{F_P} \left(\sum_{i=0}^{j-1} \frac{\omega_{n-i}((z_j X)^{q^i} - (z_j X)^{q^{i+1}})}{\pi^{i-j}} + \sum_{i=j}^{n-1} \frac{\omega_{n-i}((z_j X)^{q^i} - (z_j X)^{q^{i+1}})}{\pi^{i-j}} \right) \\ &= \exp_{F_P} \left(\sum_{i=0}^{j-1} \pi^{j-i} \omega_{n-i}((z_j X)^{q^i} - (z_j X)^{q^{i+1}}) \right) +_{F_P} \exp_{F_P} \left(\sum_{i=0}^{n-j-1} \frac{\omega_{n-j-i}((z_j X)^{q^{i+j}} - (z_j X)^{q^{i+j+1}})}{\pi^i} \right) \\ &= \mathcal{E}_{P,n-j}^Q((z_j X)^{q^j}) +_{F_P} \sum_{0 \leq i \leq j-1}^{F_P} \left(\exp_{F_P}(\pi^{j-i} \omega_{n-i} z_j X^{q^i}) -_{F_P} \exp_{F_P}(\pi^{j-i} \omega_{n-i} z_j X^{q^{i+1}}) \right) . \end{aligned} \quad (9)$$

Similarly to before, from Theorem 1 Part 1 we know that if $\pi \equiv \pi' \pmod{\mathcal{P}_K^{n+1}}$, then $\mathcal{E}_{P,n-j}^Q(X)$ is over-convergent for all $0 \leq j \leq n-1$ and therefore, $\mathcal{E}_{P,n-j}^Q((z_j X)^{q^j})$ is over-convergent for all $0 \leq j \leq n-1$. From Proposition 2.7 we know that $\exp_{F_P}(X)$ converges on the disc $\{x \in \mathbb{C}_p : v_p(x) > 1/e_K(q-1)\}$. Therefore, all the power series in (9) are over-convergent. Also all the power series in (9) have positive valuations when evaluated at 1, so we can use formal group operations on these values. Evaluating (9) at 1 we get $\mathcal{E}_{P,n-j}^Q(z_j)$. Combining this with (7) we then get

$$\left[\sum_{i=0}^{n-1} z_i \pi^i \right]_P (\mathcal{E}_{P,n}^Q(1)) = \mathcal{E}_{P,n}^Q(z_0) +_{F_P} \mathcal{E}_{P,n-1}^Q(z_1) +_{F_P} \dots +_{F_P} \mathcal{E}_{P,1}^Q(z_{n-1}) .$$

■

3.3 Local Galois module structure in weakly ramified extensions

As mentioned in the introduction, one of the main motivations for the generalisation of Dwork and Pulita's power series has come from recent progress with open questions on Galois module structure.

First, let E/F be a finite odd degree Galois extension of number fields, with Galois group G and rings of integers \mathcal{O}_E and \mathcal{O}_F . From Hilbert's formula for the valuation of the different $\mathfrak{D}_{E/F}$ ([21], IV, §2, Prop.4), we know that the valuation of $\mathfrak{D}_{E/F}$ will be even at every prime ideal of \mathcal{O}_E and we can define the square-root of the inverse different $\mathcal{A}_{E/F}$ to be the unique fractional \mathcal{O}_E -ideal such that

$$\mathcal{A}_{E/F}^2 = \mathfrak{D}_{E/F}^{-1} .$$

Erez has proved that $\mathcal{A}_{E/F}$ is locally free over $\mathcal{O}_F[G]$ if and only if E/F is at most weakly ramified, *i.e.*, the second ramification groups are trivial at every prime [6] ; however, the question of whether $\mathcal{A}_{E/F}$ is free over $\mathbb{Z}[G]$ still remains open. The tame

case has been solved by Erez [6]. Now, it is possible for weakly ramified extensions to be wildly ramified, and here new obstructions arise.

Using Fröhlich's classic *Hom-description* approach, see [8], it is possible to reduce this problem to carrying out calculations at a local level. The key to these local calculations is to have an explicit description of an integral normal basis generator for the square-root of the inverse different in weakly ramified extensions of local fields. It is also possible to reduce this problem further to considering only totally ramified extensions (see [6, §6] and [18, §3]).

Precisely, let M be the unique degree p extension of \mathbb{Q}_p contained in $\mathbb{Q}_p(\zeta_{p^2})$; this extension is totally, weakly and wildly ramified. First, in [5], Erez proves that the element

$$\frac{1 + \text{Tr}_{\mathbb{Q}_p(\zeta_{p^2})/M}(\zeta_{p^2})}{p}$$

is an integral normal basis generator for the square-root of the inverse different of M/\mathbb{Q}_p . In [23], Vinatier uses Erez's basis to prove that $\mathcal{A}_{E/F}$ is free over $\mathbb{Z}[G]$ with $F = \mathbb{Q}$ whenever the decomposition group at every wild place is abelian. Then, in [16], Pickett uses the trace map and special values of Dwork's power series to generalise Erez's basis to degree p extensions of an unramified extension of \mathbb{Q}_p that are contained in certain Lubin-Tate extensions. In [18], Pickett and Vinatier use Pickett's bases to prove that $\mathcal{A}_{E/F}$ is free over $\mathbb{Z}[G]$ under certain conditions on both the decomposition groups and base field.

Following these results, we shall give explicit descriptions of integral normal basis generators for the square-root of the inverse different in abelian totally, weakly and wildly ramified extensions of any finite extension of \mathbb{Q}_p .

Another application is concerned with the Galois module structure of the valuation ring over its associated order in extensions of local fields. Precisely, let L/K be a finite Galois extension of p -adic fields, with Galois group G . We denote by $\mathcal{O}_K \subset \mathcal{O}_L$ the corresponding valuation rings, and by $\mathfrak{A}_{L/K}$ the associated order of \mathcal{O}_L in the group algebra $K[G]$, that is

$$\mathfrak{A}_{L/K} = \{\lambda \in K[G] : \lambda \mathcal{O}_L \subset \mathcal{O}_L\}.$$

This is an \mathcal{O}_K -order of $K[G]$, and the unique one over which \mathcal{O}_L could be free as a module. When the extension L/K is at most tamely ramified, the equality $\mathfrak{A}_{L/K} = \mathcal{O}_K[G]$ holds, and \mathcal{O}_L is $\mathfrak{A}_{L/K}$ -free according to Noether's criterion. But when wild ramification is permitted, the structure of \mathcal{O}_L as an $\mathfrak{A}_{L/K}$ -module is much more difficult to determine (see, e.g., [22] for an exposition of recent progress in this topic). A p -adic version of Leopoldt's theorem asserts that the ring \mathcal{O}_L is $\mathfrak{A}_{L/K}$ -free whenever $K = \mathbb{Q}_p$ and G is abelian. However, the field \mathbb{Q}_p is actually the only base field which satisfies this property. One extension of this result is due to Byott ([2], Cor. 4.3): If L/K is an abelian extension of p -adic fields, then \mathcal{O}_L is free as a module over its associated order $\mathfrak{A}_{L/K}$ whenever the extension L/K is totally and weakly ramified. We shall construct explicit generators of the valuation ring over its associated order in maximal abelian totally, weakly and wildly ramified extensions of K , using the description of such extensions that comes from Proposition 3.1 below.

These applications are closely related to each other. Their content is resumed in Theorem 2, which we prove in this section.

Again, we denote by K a finite extension of \mathbb{Q}_p , with valuation ring \mathcal{O}_K , maximal ideal \mathcal{P}_K , and residue field k . We write $\text{card}(k) = q$. Let π be a uniformising parameter of K . By standard theory we know that the Lubin-Tate extension $K_{\pi,2}/K$ is abelian and that $[K_{\pi,2} : K] = q(q-1)$. We can therefore define $M_{\pi,2}$ as the unique sub-extension of $K_{\pi,2}/K$ such that $[M_{\pi,2} : K] = q$. The following result is a direct consequence of Theorem 1.1 of [17], however the present paper was not published at the time of writing, so we include another proof.

Proposition 3.1 *Every maximal abelian totally, wildly and weakly ramified extension of K is equal to $M_{\pi,2}$ for some uniformising parameter π .*

Proof. Let M be an abelian totally, wildly and weakly ramified extension of K . From [2, Lemma 4.2], M must be contained in $K_{\pi,2}$ for some π . Since it is of degree a power of p over K , it is thus contained in $M_{\pi,2}$.

Now, the extension $M_{\pi,2}/K$ is clearly abelian totally and wildly ramified. We are thus left with proving that it is weakly ramified. Since this extension is totally and wildly ramified, the numbers -1 and 0 are neither lower jumps, nor upper jumps. By standard Lubin-Tate theory (see [11], §7), we know that the jumps of $K_{\pi,2}/K$ occur at 0 and 1 in the upper numbering. Therefore, by Herbrand's theorem, 1 is the only upper jump (and so lower jump) of $M_{\pi,2}/K$, as required. ■

We can now prove Theorem 2.

Proof of Theorem 2. As $M_{\pi,2}/K$ is totally ramified and of degree q , we know that $e(M_{\pi,2}/K) = q$. Therefore, from [2, Theorem 1] we know that any element of $M_{\pi,2}$ with valuation 1 must be a generator of $\mathcal{O}_{M_{\pi,2}}$ over its associated order in $M_{\pi,2}/K$, and from [24, Corollary 2.5(i)] that any element of $M_{\pi,2}$ with valuation $1 - q$ must be an integral normal basis generator for $\mathcal{A}_{M_{\pi,2}/K}$. Therefore, it suffices to prove that the trace element $\text{Tr}_{K_{\pi,2}/M}(\mathcal{E}_{P,2}^Q(1))$ is a uniformising parameter of $M_{\pi,2}$.

First, the polynomial $f(X) := \frac{P(P(X))}{P(X)}$ is of degree $q(q-1)$, and it is irreducible since it is Eisenstein over K : Indeed, $f(X) = P(X)^{q-1} + \sum_{i=2}^{q-1} a_i P(X)^{i-1} + \pi$ and each a_i is divisible by π because P is a Lubin-Tate polynomial. Therefore, since $f(\mathcal{E}_{P,2}^Q(1)) = 0$, f is the minimal polynomial of $\mathcal{E}_{P,2}^Q(1)$. Thus, $\text{Tr}_{K_{\pi,2}/K}(\mathcal{E}_{P,2}^Q(1))$ is the coefficient of $X^{q(q-1)-1}$ in $f(X)$, i.e., $\text{Tr}_{K_{\pi,2}/K}(\mathcal{E}_{P,2}^Q(1)) = (q-1)a_{q-1}$. In particular, $\text{Tr}_{K_{\pi,2}/K}(\mathcal{E}_{P,2}^Q(1))$ has valuation 1 in K .

Now, we denote by d the valuation of the different of the extension $M_{\pi,2}/K$. According to the characterisation of the different [21, Ch. III, §3, Prop. 7], we have

$$\forall i \in \mathbb{Z}, \quad \text{Tr}_{M_{\pi,2}/K}(\mathcal{P}_{M_{\pi,2}}^{-2d+i}) = \mathcal{P}_K^{\lfloor \frac{i}{e_{M_{\pi,2}/K}} \rfloor},$$

where $\lfloor x \rfloor$ denotes the largest integer n with $n \leq x$.

Since the extension $M_{\pi,2}/K$ is totally and weakly ramified of degree q , we have $d = 2(q - 1)$, by Hilbert's formula for the valuation of the different. In particular, for $i = 2q - 1$, the previous relation gives the identity $Tr_{M_{\pi,2}/K}(\mathcal{P}_{M_{\pi,2}}) = \mathcal{P}_K$, and for $i \geq 2q$, it proves that $Tr_{M_{\pi,2}/K}(\mathcal{P}_{M_{\pi,2}}^2) \subseteq \mathcal{P}_K^2$.

On the other hand, since the extension $K_{\pi,2}/M_{\pi,2}$ is tamely ramified, and because $\mathcal{E}_{P,2}^Q(1)$ is a uniformising parameter of $K_{\pi,2}$ by Theorem 2, we know that the element $Tr_{K_{\pi,2}/M_{\pi,2}}(\mathcal{E}_{P,2}^Q(1))$ lies in $\mathcal{P}_{M_{\pi,2}}$.

Now, from the transitivity of the trace we also have

$$Tr_{K_{\pi,2}/K}(\mathcal{E}_{P,2}^Q(1)) = Tr_{M_{\pi,2}/K}(Tr_{K_{\pi,2}/M_{\pi,2}}(\mathcal{E}_{P,2}^Q(1))) ,$$

and so, we can conclude that $Tr_{K_{\pi,2}/M_{\pi,2}}(\mathcal{E}_{P,2}^Q(1))$ is indeed a uniformising parameter in the field $M_{\pi,2}$. ■

We shall close this paper with the following corollary to Theorem 2, which gives explicit integral normal basis generators for the square root of the inverse different in every abelian totally, wildly and weakly ramified extensions of K .

Corollary 3.2 [Corollary to Theorem 2] *Let M be an intermediate subfield of the extension $M_{\pi,2}/K$. Let $\alpha_{\pi,2}$ equal either $\frac{Tr_{K_{\pi,2}/M}(\mathcal{E}_{P,2}^Q(1))}{\pi}$ or $\frac{Tr_{K_{\pi,2}/M}(\mathcal{E}_{P,2}^Q(1))+q}{\pi}$. Then, $\alpha_{\pi,2}$ is an integral normal basis generator for $\mathcal{A}_{M/K}$.*

Proof. This follows directly from Theorem 2 and ([24], Corollary 2.5(ii)). ■

References

- [1] N. Bourbaki. *Algèbre commutative*. Masson, Paris, 1983.
- [2] N. P. Byott. Integral Galois Module Structure of Some Lubin-Tate Extensions. *J. Number Theory*, 77:252–273, 1999.
- [3] E. J. Ditters. Formale gruppen, die vermutungen von atkin-swinnerton-dyer und verzweigte witt-vektoren. *Lecture Notes, Göttingen*, 1975.
- [4] V. G. Drinfel'd. Coverings of p -adic symmetric domains. *Funkcional. Anal. i Priložen.*, 10(2):29–40, 1976.
- [5] B. Erez. The Galois Structure of the Trace Form in Extensions of Odd Prime Degree. *J. Algebra*, 118:438–446, 1988.
- [6] B. Erez. The Galois Structure of the Square Root of the Inverse Different. *Math.Z.*, 208:239–255, 1991.

- [7] A. Fröhlich. *Formal Groups*. Number 74 in Lecture Notes in Math. Springer Verlag, New York, 1968.
- [8] A. Fröhlich. *Galois Module Structure of Algebraic Integers*. Springer-Verlag, 1983.
- [9] M. Hazewinkel. *Formal groups and applications*, volume 78 of *Pure and Applied Mathematics*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1978.
- [10] M. Hazewinkel. Twisted Lubin-Tate formal group laws, ramified Witt vectors and (ramified) Artin-Hasse exponentials. *Trans. Amer. Math. Soc.*, 259(1):47–63, 1980.
- [11] K. Iwasawa. *Local Class Field Theory*. Oxford University Press, 1986.
- [12] J.-M. Fontaine L. Fargues. Courbes et fibrés vectoriels en théorie de hodge p -adique. *preprint*, 2011.
- [13] S. Lang. *Algebra*. Addison-Wesley, 1965.
- [14] S. Lang. *Cyclotomic Fields II*. Springer-Verlag, New York, 1980.
- [15] J. Lubin and J. Tate. Formal complex multiplication in local fields. *Ann. of Math. (2)*, 81:380–387, 1965.
- [16] E. J. Pickett. Explicit Construction of Self-Dual Integral Normal Bases for the Square-Root of the Inverse Different. *J. Number Theory*, 129:1773 – 1785, 2009.
- [17] E. J. Pickett and S. Vinatier. Exponential Power Series, Galois Module Structure and Differential Modules. Submitted.
- [18] E. J. Pickett and S. Vinatier. Self-Dual Integral Normal Bases and Galois Module Structure. Submitted.
- [19] A. Pulita. Rank one solvable p -adic differential equations and finite abelian characters via Lubin-Tate groups. *Math. Ann.*, 337(3):489–555, 2007.
- [20] J. P. Serre. Local class field theory. In J. W. S. Cassels and A. Fröhlich, editors, *Algebraic Number Theory*, London, 1967. Academic Press.
- [21] J. P. Serre. *Corps Locaux*. Hermann, Paris, 1968.
- [22] L. Thomas. On the Galois module structure of extensions of local fields. *Publ. Math. Besançon*, pages 157–194, 2010. Actes de la Conférence “Fonctions L et Arithmétique”.
- [23] S. Vinatier. Structure galoisienne dans les extensions faiblement ramifiées de \mathbb{Q} . *J. Number Theory*, 91(1):126–152, 2001.
- [24] S. Vinatier. Galois Module Structure in Weakly Ramified 3-Extensions. *Acta Arith.*, 119(2):171–186, 2005.
- [25] L. C. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.
- [26] E. Witt. Zyklische körper und algebren der charakteristik vom grad p^n . *J. Reine Angew. Math.*, 174:126–140, 1936.